



TECHNICAL BRIEF · BASED ON GAO-23-106701 · DHS

NONE OF 7 DHS PROGRAMS COMPLETED A CYBER RISK MEMO AT DECISION EVENTS

0 of 7

DHS MAJOR ACQUISITION PROGRAMS THAT COMPLETED A CYBERSECURITY RISK
RECOMMENDATION MEMORANDUM AT A DECISION EVENT HELD AFTER THE JULY 2020
INSTRUCTION, PER GAO'S 2023 REVIEW

In April 2023, GAO found that none of seven DHS programs with decision events after July 2020 completed the required cybersecurity risk memo. GAO told DHS to say which programs need one and when exemptions apply, and the recommendation was open as of GAO's last update.

THE FINDING

In April 2023, GAO published [DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification](#) (GAO-23-106701). GAO reviewed 25 DHS major acquisition programs. Most of the report covers cost and schedule baselines, and one section covers cybersecurity.

DHS Instruction 102-01-012, *Cybersecurity through the Acquisition Lifecycle Framework*, issued in July 2020, requires major programs to present a cybersecurity risk recommendation memorandum (CRRM) at acquisition decision events (ADEs). A CRRM states the program's cybersecurity status and a high, medium, or low risk recommendation, and the DHS Chief Information Security Officer signs it out.

None of the seven programs that held ADEs after the instruction completed one. One showed GAO a DHS waiver. The other six said they used other documentation, that a CRRM did not apply, or that they did not develop one.

GAO recommended that DHS, as it updates the instruction, clarify "(1) which major acquisition programs are required to have completed cybersecurity risk recommendation memorandums prior to acquisition decision events, and (2) when exemptions apply." DHS concurred. GAO also made one nonpublic recommendation in a sensitive version of the report.

WHY IT KEEPS HAPPENING

The instruction left three questions open, according to GAO: when the CRRM requirement can be waived, when it does not apply, and what other documentation can stand in for it. Programs answered those questions one at a time. GAO warned that without clear exemption rules, "programs may not prepare the memorandums when they are needed," and that DHS may then lack the information to assess cybersecurity risk and confirm that mitigations are adequate.

The fix has moved slowly. DHS told GAO in 2023 that it planned to implement the recommendation by March 30, 2024. GAO's status notes say DHS added CRRM completion as a required document for all major programs in its primary acquisition instruction, 102-01-001, in January 2023. In April 2025, DHS's Office of Program Accountability and Risk Management said the revision would specify which programs need the memos and when exemptions apply, with completion planned for December 2025.

WHY IT MATTERS TO YOUR BID

Evaluators on DHS major-program cyber and authorization requirements can read GAO-23-106701. They know that a CRRM is a risk call with a status line behind it, and that both rest on records a contractor keeps.

A technical volume that treats the memo as a document to be typed before a milestone reads thin. A stronger volume shows how the offeror keeps the underlying record ready on the date a decision event is called. It also says what the offeror does when a program office believes an exemption applies, because that was where all seven programs ended up.

Timing matters too. If DHS finalizes its revision, exemptions will be written down. A bid that ties its method to the instruction as published on the solicitation date, and shows how it adapts when the instruction changes, answers the risk an evaluator is most likely to probe.

TECHNICAL APPROACH

The method comes from Avalon's [NIST RMF Implementation service](#). It describes how the work is done, at the methodology level, for one program at a time in unclassified environments. The CISO signs the CRRM and the Authorizing Official makes the authorization decision. Avalon does neither.

- 1. Build the posture calendar behind each decision event.** For each program, list the planned ADE dates and record the RMF state behind each one: package age, ATO status and expiration date, GRC record health, open POA&M items, and prior assessment findings. The output is a dated gap list showing which evidence will be stale on which ADE.
- 2. Validate the impact level the risk rating rests on.** Confirm the [FIPS 199](#) categorization using SP 800-60 information types, then the [NIST SP 800-53B](#) baseline and its documented organization-defined parameters. A high, medium, or low recommendation is hard to defend if the categorization behind it is undocumented.
- 3. Separate inherited controls from program-owned ones.** Build the customer responsibility matrix for controls inherited from shared DHS services or a FedRAMP-authorized cloud, and check each against the providing system's package. The program's risk statement then covers what the program owns.
- 4. Define cybersecurity status as monitoring data.** Write the ISCM strategy under [NIST SP 800-137](#): metrics, monitoring frequency per control, data feeds from scanners and configuration tools, and the reporting cadence. "Current status" at an ADE then comes from a feed with a date on it, not from a narrative rewritten for the milestone.
- 5. Map substitute documents against the same record.** For a program that cites a waiver, an inapplicability finding, or other documentation, compare that documentation to the elements in steps 1 through 4 and mark

what it covers and what it does not. The map goes to the program's ISSM. Whether the substitute is accepted stays with DHS.

All five steps work inside [NIST SP 800-37 Rev. 2](#), which supports authorization decisions based on continuous monitoring.

WHAT "FIXED" LOOKS LIKE

GAO closes the recommendation on DHS action, not contractor action. The evidence is an updated DHS instruction that says which major programs must complete a CRRM before ADEs and when exemptions apply. GAO's own notes show the department was working toward that revision.

At the program level, these are targets, not GAO criteria:

- Every planned ADE shows either a completed CRRM or a written exemption citing the instruction.
- No ADE is held with neither.
- The impact level, baseline, and inherited-control matrix in the GRC record are dated and match the system.
- Cybersecurity status for the memo comes from monitoring feeds refreshed within the strategy's cycle.
- Each substitute document has a gap map reviewed by the ISSM.

STATUS CHECK

OPEN Open as of GAO's last update, April 2025. GAO lists the recommendation as open and partially addressed, and its product page shows no last-updated date. DHS planned to complete the instruction revision in December 2025, and the page did not show that revision as complete when Avalon read it in October 2026. The sensitive recommendation is not public and is not covered here.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Decision-event posture calendar, FIPS 199 and SP 800-53B baseline validation, inherited-control matrix, ISCM status metrics, and a substitute-document gap map under the prime's A&A or program-office cyber support task order, in unclassified environments
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA MAS (SIN 54151S IT Professional Services); GSA Alliant 3

If DHS major-program cyber or authorization support is in your capture plan, Avalon teams as the sub that keeps each program's categorization, inheritance, and monitoring records dated and ready, so the prime can put evidence in front of the CISO at every decision event.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.